1-1-2002

Exploring Internet Privacy through Cable Broadband Struggles: ISPs walk a Fine Line Between Privacy and Security

Cyndie Chang

NOTES & COMMENTS

EXPLORING INTERNET PRIVACY THROUGH CABLE BROADBAND STRUGGLES: ISPs WALK A FINE LINE BETWEEN PRIVACY AND SECURITY

I. INTRODUCTION

Imagine a computer user logging onto the Internet using his cable Internet service provider ("ISP"). When he recently subscribed to the service, he accepted the provider's privacy statement by clicking on "I accept" with his mouse. What he does not know is that the government now has access to his confidential information without his consent or notice.[1] Such information includes the scope of his Internet use, the duration of his use, his social security number, his credit card and bank account number, and other identifying information.[2] By the simple act of subscribing, all this personal information becomes subject to disclosure to the government.

Since the advent of broadband Internet access provided over cable television lines ("cable broadband"), privacy regulation has been subject to constant change. With the recent enactment of the USA Patriot Act ("USAPA"),[3] privacy protections afforded to cable Internet users have substantially decreased. Before the terrorist attacks of September 11, 2001, the Cable Communications Policy Act of 1984 ("Cable Act") required cable companies to notify and grant a hearing to cable subscribers when their confidential information was subject to disclosure to the government.[4] However, the USAPA has changed the law so that those rights are now

1. *See* 18 U.S.C.S. § 2703 (2001).

2. *In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D), 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001); John Reynolds & Amy Worlton, *USA Patriot Act Calls for Privacy Policy Review*, METROPOLITAN CORP. COUNS., Jan. 2002, at 7; *see* 18 U.S.C.S. § 2703.

3. USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 224, 115 Stat. 272, 283–85, 295 (2001).

4. 47 U.S.C. § 551 (1994), *amended by* USA Patriot Act § 211; *see In re Application of the United States*, 157 F. Supp. 2d at 288 (finding notification of and hearing for cable Internet subscribers was statutorily ambiguous).

unavailable to cable broadband subscribers.[5]

Furthermore, the USAPA expanded the scope of information the government could obtain from ISPs.[6] This Comment addresses the personal information the government can obtain from customer subscription records. This includes "non-content" information, i.e., personal identifying information the company uses in its normal course of business,[7] and "content" information, i.e., information in which a person has a reasonable expectation of privacy, such as the contents of communications and activities online.[8] In addition, the USAPA also has a provision for ISPs to voluntarily disclose subscriber's personal information to the government.[9] Thus, some of the USAPA's provisions threaten civil liberties by granting broad governmental powers in using private information culled from one's Internet subscription.[10]

The terrorist attacks have shifted American focus from privacy to the need for security.[11] Consequently, Congress has enacted rapid changes to Internet privacy protections.[12] The USAPA goes too far by giving federal investigators too much information too easily. However, with the increasing availability of information on the Internet, there will eventually be a demand once again for online privacy. When that time comes, Congress may regret enacting this legislation.

This Comment explores the current scope of Internet privacy protection of Internet users' confidential information via cable broadband service. It further examines how the USAPA has amended past problems with cable broadband privacy regulations, which has created future privacy concerns. Part II provides a background of the development of cable broadband and pertinent federal legislation. Part III discusses the legal treatment of cable broadband and how the Federal Communications

---

5. *See* USA Patriot Act §§ 210–211.

6. *See Id.* §§ 209–212.

7. *In re Application of the United States*, 157 F. Supp. 2d at 288; *see* Susan Brenner, *Article IV—Obtaining Evidence: Interception & Surveillance*, in MODEL CODE OF CYBERCRIMES INVESTIGATIVE PROCEDURE, *at* http://cybercrimes.net/MCCIP/art4.htm (last visited Feb. 7, 2002) (model code drafted by students of the 2000 Cybercrimes Seminar at the University of Dayton School of Law) (noting names, addresses, phone numbers, and birthdays as examples of "non-content" information).

8. *See* Brenner, *supra* note 7; *see* Brock N. Meeks, *Rolling Up Freedoms in a New Nation*, MSNBC.COM (Nov. 14, 2001), *at* http://www.msnbc.com/news/657173.asp (noting the contents of the "to" and subject lines of emails as examples of "non-content" information).

9. 18 U.S.C.S. § 2702(b)(6) (2001).

10. *See* USA Patriot Act §§ 209–212.

11. *See* Michael Bartlett, *Americans Still Guard Telephone, E-mail Privacy-Study*, *at* http://www.newsbytes.com/news/01/170291.html (last visited Sept. 19, 2001).

12. *See id.*

Commission ("FCC") has handled cable broadband. Part IV examines the recent developments pursuant to the USAPA that affect cable broadband subscribers' records. Part V evaluates the balance between privacy and security. Part VI concludes that the current state of law in this area needs reexamination and reform, such as establishing greater privacy protections for Internet users' personal information.

II. BACKGROUND AND HISTORICAL DEVELOPMENT OF CABLE BROADBAND AND INTERNET PRIVACY

With increasing globalization, the Internet will be the most efficient means of communication.[13] Internet use is predicted to grow 119% between 2000 and 2005.[14] By 2010, the world may conduct a quarter of all global commerce on the Internet.[15] Most early connection to the Internet occurred over standard telephone lines.[16] Now, technology developed in the past decade has advanced Internet connection speed and quality by using cable broadband and digital subscriber lines ("DSL").[17]

The privacy protections afforded to cable broadband subscribers are subject to debate.[18] The most current Federal Trade Commission ("FTC") report on the state of Internet privacy urged Congress to safeguard consumer privacy on the Internet.[19] In addition, in a poll conducted before the September 11 attacks, Americans feared there was insufficient protection of their privacy on the Internet.[20] Fifty-seven percent of Americans wanted Congress to pass legislation governing the use of

13. Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 ALB. L.J. SCI. & TECH. 1, 26 (2001); *see* Sen. Ernest F. Hollings, *Individual Privacy on the Internet*, PRIVACY NEWSLETTER (Mintz Levin Cohn Ferris Glovsky and Popeo PC), Aug. 2001, at 2 (citing prediction by John Chambers of Cisco Systems). "[T]he Internet economy is projected to reach $2.8 trillion by 2003." Rueda, *supra*, at 28.

14. Rueda, *supra* note 13, at 25–26.

15. Hollings, *supra* note 13, at 2.

16. *See* Milo Medin & Jay Rolls, *The Internet via Cable*, SCI. AM., Oct. 1999, at 100.

17. *See* Christopher Heitman, *High-Speed Internet Connections What's Best for Your Firm?*, GPSOLO, Dec. 2001, at 24–25.

18. *See In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D), 157 F. Supp. 2d 286 (S.D.N.Y. 2001). *See generally EFF Analysis of the Provisions of the USA Patriot Act that Relate to Online Activities*, Electronic Frontier Foundation, *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (Oct. 31, 2001).

19. Hollings, *supra* note 13, at 1.

20. *Id.* (citing a poll from *Business Week*); Rueda, *supra* note 13, at 31 (citing survey that showed seventy-three percent of U.S. consumers were anxious about credit card purchases over the Internet).

personal information on the Internet.[21] In addition, only fifteen percent of Americans polled desired government deference to voluntary, industry-developed privacy regulations in this area.[22] Since the terrorist attacks, a new perspective on Internet privacy has arisen.[23] Americans now demand more security in fear of future terrorism.[24] Benjamin Franklin once advised, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."[25] Thus, this democracy has easily accepted a bill that now puts personal information given to ISPs at the fingertips of federal investigators—the USAPA.[26]

A. The Development of Cable Broadband

The FCC defines "broadband" as the "evolving digital technologies that provide consumers a signal switched facility offering integrated access to voice, high-speed data service, video[-on]-demand services, and interactive delivery services."[27] Broadband is unique in that it is the only means to reliably deliver real-time streaming video, Internet-based videoconferencing, and access to a remote local network.[28] Broadband technologies, such as fiber optics, began in the 1950s.[29] By the 1990s, there was a great demand for high-speed data, voice, and video among business and residential Internet users.[30]

Because of the great reach of television, hybrid fiber coaxial cable is the preferred conduit for residential broadband.[31] As of June 2000, there were about 3.12 million residential broadband subscribers in the United States, nearly seventy percent of which were cable broadband subscribers.[32]

---

21. Hollings, *supra* note 13, at 1.

22. *Id.*

23. Bartlett, *supra* note 11.

24. *Id.*

25. Rachel King & Lamar Smith, *Symposium: Q: Is Congress Giving Too Much Surveillance Power to Federal Law Enforcement?*, INSIGHT ON NEWS, Jan. 14, 2002, *at* http://www.insightmag.com/main.cfm/include/detail/storyid/160718.html (citing the negative response of Lamar Smith).

26. *See* USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 224, 115 Stat. 272, 283–85, 295 (2001).

27. *Glossary of Telecommunications Terms*, *at* http://www.fcc.gov/glossary.html (last visited Jan. 15, 2002).

28. Jim Chen, *The Authority to Regulate Broadband Internet Access over Cable*, 16 BERKELEY TECH. L.J. 677, 678 (2001).

29. Anthony Palazzo, *History of the Broadband Industry*, *at* http://www.broadband-internet.org/history.htm (last visited Jan. 15, 2002).

30. *Id.*

31. Chen, *supra* note 28, at 679.

32. *Id.*

For example, in 2001 Cablevision provided cable television to three million customers and at least 367,000 Optimum Online (cable broadband) customers.[33] Hence, the consumer market creates a tremendous need for high speed Internet access through cable companies, such as Road Runner and Excite@Home.com.[34]

Phone companies who offer high-speed Internet access through DSL services come in a distant second place.[35] Internet access could be up to 100 times faster through a cable modem than the traditional dial-up connection.[36] There are also satellite or fixed wireless technologies that provide Internet access.[37] However, these services remain unpopular due to problems with line-of-sight requirements, weather-related issues of reliability, and reliance on telephone lines for the return path.[38]

Internet access over a cable line uses a coaxial cable, which can carry hundreds of megahertz ("MHz") of signals depending on the space or bandwidth of the cable.[39] Six MHz is all that is required to receive a television channel or to get downstream data—data from the Internet to a single computer.[40] Two MHz is all that is required for upstream data—information sent from a person back to the Internet.[41]

Getting the benefits of cable broadband is simple. All the equipment needed is a cable modem for the customer and a Cable Modem Termination System (CMTS) for the cable company.[42] These cable lines are the connection to the cable companies.[43] Some cable companies send transfer signals from the companies' central facility (the "head end") via optical fibers.[44] The head end connects to a network neighborhood area ("the node"), which is a network of coaxial cable.[45] This familiar coaxial

33. Harry Berkowitz, *Ruling Limits Online Privacy; Cablevision Must Disclose Customer Info*, NEWSDAY, Aug. 24, 2001, at A8.

34. *The Broadband Industry*, *at* http://www.broadband-internet.org (last visited Jan. 15, 2002). Excite@Home recently ceased operations. Alorie Gilbert & Rachel Konrad, *Book Closes on Excite@Home*, CNET NEWS.COM (Feb. 28, 2002), *at* http://news.com.com/2100-1033-848197.html.

35. *Id.*

36. Medin & Rolls, *supra* note 16.

37. Chen, *supra* note 28, at 679.

38. *Id.*

39. *See How Cable Modems Work*, Marshall Brain's HowStuffWorks, *at* http://www.howstuffworks.com/cable-modem.htm/printable (last visited Jan. 15, 2002).

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. Medin & Rolls, *supra* note 16.

45. *Id.*

cable runs from the node to a person's home television or set-top box to deliver the signal.[46] In other cable systems, coaxial cable is the only medium for distributing signals.[47] Consequently, cable companies greatly expanded their services when they moved from providing television services to providing Internet services as well.[48]

B. The Cable Communications Policy Act of 1984

The Cable Act amended the Communications Act of 1934.[49] The Cable Act establishes general cable regulations and privacy protections for its subscribers, including restrictions on the disclosure, maintenance, and collection of subscriber information.[50] For instance, cable companies cannot collect "personally identifiable information"[51] without the subscriber's prior consent unless this information is necessary to render service or detect unauthorized reception.[52] The other regulatory provisions of the Cable Act include establishment of cable franchises,[53] renewal of the franchises,[54] standards for local regulation of cable companies,[55] and encouragement of diversity in cable content.[56]

The Cable Act requires notification to the subscriber as to how and why his personal information is subject to collection and disclosure.[57] The cable operator shall provide notice that clearly and conspicuously informs the subscriber how his personally identifiable information is collected.[58] Courts interpreted the requirement for "clear and conspicuous" language required for notice provisions to mean that any subscriber "could

46. *Id.* Each network neighborhood area typically encompasses about 1,000 homes. *Id.*

47. *How Cable Modems Work*, *supra* note 39.

48. *See* Medin & Rolls, *supra* note 16.

49. *CDT's Guide to Online Privacy*, Center for Democracy and Technology, *at* http://www.cdt.org/privacy/guide/protect/laws.html (last visited Jan. 15, 2002). The Communications Act of 1934 created a "blanket prohibition against the interception of communications, with no exception for law enforcement." Mark G. Young, Note, *What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance*, 70 FORDHAM L. REV. 1017, 1057 (2001).

50. *See generally* 47 U.S.C.S. § 551 (2001).

51. *Id.* § 551(a)(2) (stating that "personally identifiable information" does not include any record of aggregate data that does not identify particular persons).

52. *Id.* § 551(b).

53. *Id.* § 541.

54. *Id.* § 546.

55. *Id.* §§ 543–544.

56. 47 U.S.C.S. §§ 531–532 (2001).

57. *Id.* § 551.

58. *Id.* § 551(a).

reasonably be expected to have . . . understood its meaning."[59]

Therefore, the subscriber will know the *nature* of the personally identifiable information, the *purpose* of the disclosure, the *frequency* with which the information will be collected, the *time period* of these collections, the *time and place* of access to this information, the *limitations* of this collection and disclosure, an *identification* of the types of persons to whom the disclosure may be made, and the *enforcement* of these regulations.[60] Civil remedies are available to enforce these standards.[61] A cable company can be subject to actual damages, punitive damages, reasonable attorney's fees, and any other lawful remedies available to a cable subscriber.[62]

Most importantly, cable companies cannot disclose personally identifiable information to third parties without consent subject only to four exceptions.[63] The first exception allows disclosure in order to render cable service to the subscriber.[64] The second exception is disclosure pursuant to a legitimate court order if the cable company notifies the subscriber of such order and the subscriber has an opportunity to appear and contest the court order.[65] The third exception is disclosure of the names and addresses of the subscriber to any other services when the subscriber has the opportunity to limit such disclosure and the disclosure does not reveal, directly or indirectly, the extent of viewing or other use by the subscriber or the nature of any transactions made by the subscriber.[66] The fourth exception allows disclosure to a government authority under certain situations, but such disclosure does not include records revealing cable subscribers' selections of video programming.[67]

---

59. Scofield v. Telecable of Overland Park, 973 F.2d 874, 880 (10th Cir. 1992).

60. 47 U.S.C.S. § 551(a).

61. *Id.* § 551(f).

62. *See id.* § 551(f)(2)–(3).

63. *See id.* § 551(c)(2).

64. *Id.* § 551(c)(2)(A) (stating disclosure "necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber").

65. *Id.* § 551(c)(2)(B) (stating disclosure "subject to subsection (h), made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed"); *see also* discussion *infra* Part IV.A.

66. 47 U.S.C.S. § 551(c)(2)(C) (2001).

67. *Id.* § 551(c)(2)(D); *see also* discussion *infra* Part IV.A (comparing provisions for government disclosure numbers second and fourth exceptions).

C. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act ("ECPA")[68] is aimed at all providers of electronic communication service, including electronic mail operations, computer data transmissions, cellular phones, and paging devices.[69] In particular, the ECPA addresses services that provide users thereof "the ability to send or receive wire or electronic communications."[70] Prevailing decisional law has established that all ISPs fall within the ECPA, including cable ISPs.[71]

In 1986, the ECPA expanded the scope of existing federal wiretap laws to provide protection for electronic communications.[72] The ECPA was an expansion of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which had governed telephone communications.[73] Congress amended Title III to conform to developing communications and computer technology.[74] For instance, the ECPA expanded already existing federal privacy protections by broadening the scope of "privileged communications to include all forms of electronic transmissions, such as video, text, audio, and data."[75]

The ECPA provides that a governmental entity can obtain subscriber records and personal information through the following ways:[76] a warrant;[77] a court order;[78] the consent of the subscriber or customer to such disclosure;[79] a formal written request relevant to a law enforcement

68. 18 U.S.C.S. §§ 2701–2703 (2001).

69. *Electronic Communications Privacy Act*, Jones Telecommunications & Multimedia Encyclopedia, *at* http://www.digitalcentury.com/encyclo/update/ecpa.html (last visited Jan. 15, 2002).

70. 18 U.S.C. § 2510(15).

71. *In re Application of the United States*, 157 F. Supp. 2d at 289; *see* Gucci Am., Inc. v. Hall & Assoc., 135 F. Supp. 2d 409, 419 n.20 (S.D.N.Y. 2001) (stating "[p]roviders of Internet services have traditionally been viewed as subject to the Electronic Communications [Privacy Act]"); *see* United States v. Kennedy, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000) ("Traditionally, Internet providers have considered themselves subject to the regulations and prohibitions set forth in the Electronic Communications Privacy Act."); *see* United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999); *see* Jessup-Morgan v. Am. Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998); *see* McVeigh v. Cohen, 983 F. Supp. 215, 219 (D.D.C. 1998).

72. *CDT's Guide to Online Privacy*, *supra* note 49.

73. *See* S. REP. NO. 99-541, at 2 (1986); *Electronic Communications Privacy Act*, *supra* note 69, *at* http://www.digitalcentury.com/encyclo/update/ecpa.html.

74. *Electronic Communications Privacy Act*, *supra* note 69.

75. *CDT's Guide to Online Privacy*, *supra* note 49.

76. 18 U.S.C.S. § 2703(c)(1) (2001).

77. *Id.* § 2703(c)(1)(A).

78. *Id.* § 2703(c)(1)(B).

79. *Id.* § 2703(c)(1)(C).

investigation;[80] an administrative subpoena for limited information;[81] or a voluntary disclosure from the ISP for emergencies.[82]

In addition, where the government seeks records related to a subscriber of the electronic communications service, the government is not required to provide notice to the subscriber.[83]

Furthermore, the government is not limited to "non-content" information, which is personal identifying information.[84] Although the ECPA generally prohibits an entity providing electronic communication service from disclosing contents of a communication while it is in "electronic storage by that service,"[85] it allows government entities to obtain "content" information under the same means described above for subscriber records.[86] These ways include a warrant without notice to the subscriber and a court order with delayed notice.[87]

Furthermore, the ECPA allows ISPs to access the information itself.[88] After the USAPA, the ECPA now allows service providers to voluntarily disclose subscriber information to the government in emergencies.[89]

D. The USA Patriot Act

President Bush signed the USAPA on October 26, 2001.[90] The bill passed in the House by a vote of 357 to 66, and in the Senate by a vote of

80. *Id.* § 2703(c)(1)(D).

81. *See id.* § 2703(c)(1)–(2). This limited information includes the following: (1) name; (2) address; (3) local and long distance telephone connection records, or records of session times and durations; (4) length of service, including start date and types of service utilized; (5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (6) means and source of payment for such service, including any credit card or bank account number of a subscriber. *Id.* § 2703(c)(2).

82. 18 U.S.C.S. § 2702(b)(6)(C) (2001).

83. *In re Application of the United States*, 157 F. Supp. 2d at 289.

84. *See generally* Brenner, *supra* note 7.

85. 18 U.S.C.S. § 2702(a).

86. *Id.* § 2703(a).

87. *Id.* § 2703(b).

88. *See id.* § 2703(a); *see also Kennedy*, 81 F. Supp. 2d at 1103. In *Kennedy*, the court found that the ECPA did not protect a subscriber's Internet activities from the cable company. *Id.* at 1110. A subscriber on the same cable network as Kennedy reported discovering Kennedy's child pornography on his hard drive. *Id.* at 1106–07. The cable company accessed the subscriber's hard drive, found the pornography, and reported this information to authorities. *Id.* The court denied Kennedy's motion to suppress the evidence accessed by the cable company. *Id.* at 1115.

89. 18 U.S.C.S. § 2703(b)(6)(C).

90. *EFF Analysis of the Provisions of the USA Patriot Act*, *supra* note 18.

98 to 1.[91] Senator Russell D. Feingold cast the only dissenting Senate vote, arguing that it would allow unconstitutional searches and punish individuals for vague associations with possible terrorists.[92] The law gives sweeping new powers to domestic law enforcement and foreign intelligence agencies.[93] Accordingly, Attorney General Ashcroft directed all ninety-four U.S. Attorneys' offices and fifty-six FBI field offices to implement the new legislation immediately.[94]

The USAPA makes changes to fifteen different statutes.[95] The Act affects areas such as online activities and surveillance, money laundering, immigration, and providing for victims of terrorism.[96] Although the Act contains 1,016 sections, the scope of this Comment will explore only the USAPA's impact on disclosure of Internet users' records to the government.[97] President Bush signed the bill because he believed that modifying existing surveillance laws on communications was another "essential tool to pursue and stop terrorists."[98] He also explained that existing laws arose out of an era of rotary telephones.[99]

President Bush believes the bill "takes account of the new realities and dangers posed by modern terrorists. It will help law enforcement to identify, to dismantle, to disrupt, and to punish terrorists before they strike."[100] In fact, the bill's title (USA PATRIOT) is an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."[101] The bill also allows intelligence and criminal operations the chance to share information rather than operating on separate tracks.[102] Thus, the Act allows for the broad sharing of sensitive information in criminal cases with intelligence

91. *The USA-Patriot Act: Congress and White House Say Goodbye to the Bill of Rights*, Chicago Independent Media Center, *at* http://chicago.indymedia.org (last visited Jan. 24, 2002).

92. Adam Clymer, *Antiterrorism Bill Passes; U.S. Gets Expanded Powers*, N.Y. TIMES, October 26, 2001, at A1.

93. *EFF Analysis of the Provisions of the USA Patriot Act*, *supra* note 18.

94. *The USA-Patriot Act: Congress and White House Say Goodbye to the Bill of Rights*, *supra* note 91.

95. *EFF Analysis of The Provisions of the USA Patriot Act*, *supra* note 18.

96. *Id.*

97. *See* USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 224, 115 Stat. 272, 283–85, 295 (2001). This Comment will focus mainly on sections 209–212, 224.

98. *Bush Comments on Signing New Antiterrorism Law*, (Oct. 26, 2001) http://usinfo.state.gov/topical/pol/terror/01102600.htm.

99. *Id.*

100. *Id.*

101. USA Patriot Act §§ 209–212.

102. *Bush Comments on Signing New Antiterrorism Law*, *supra* note 98.

agencies, including the CIA, the NSA, the INS, and the Secret Service.[103]

The bill raises various concerns. For example, most members of Congress did not have time to read the entire 342-page bill, drafted by a handful of people in secret and not subject to committee process or inter-agency review,[104] either process of which would have addressed the parts of the bill that encroached on civil liberties.[105] Furthermore, the bill lacks any formal conference report and had only one public hearing, which will make it difficult for courts to interpret legislative history if someone ever challenges the bill.[106] Because the bill lacks a true consensus, the bill was essentially "driven by the politics of the moment."[107]

In addition, the USAPA eliminated the checks and balances that previously gave courts the opportunity to curb abuses of government surveillance powers.[108] Hence, the USAPA reflects a fundamental distrust of judges because "it treats the courts as inconvenient obstacles to executive action rather than an essential instrument of accountability."[109] The broad grants of surveillance powers given to government agents is arguably overreaching because it lacks judicial oversight to assure constitutionality.[110] The consequences may show in important cases where one may challenge the constitutionality of this law and suppress evidence collected under this bill.[111]

Lastly, the provisions of the act were unnecessary because the police already had the power to obtain the essential information by going through

---

103. *USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances; An ACLU Legislative Analysis*, *at* http://www.aclu.org/congress/1110101a.html (Nov. 1, 2001) [hereinafter *USA Patriot Act Boosts Government Powers*].

104. Nat Hentoff, *Terrorizing the Bill of Rights*, VILLAGE VOICE (Nov. 9, 2001), *at* http://www.villagevoice.com/issues/0146/hentoff.php; *see EFF Analysis of The Provisions of the USA Patriot Act*, *supra* note 18.

105. Gary S. Lincenberg & Benjamin N. Gluck, *A Patriotic Critique of the PATRIOT Act: The Antiterrorism Legislation that Congress Passed in Haste is a Threat to Civil Liberties*, L.A. LAW., Feb. 2002, at 52.

106. Hentoff, *supra* note 104; *see* Press Release, American Civil Liberties Union, Bush Signs Sweeping Law Enforcement Bill (Oct. 26, 2001), *at* http://www.aclu.org/news/2001/n102601a.html.

107. Interview with Ari Schwartz, Associate Director for the Center for Democracy and Technology (Oct. 30, 2001), *at* http://www.cnn.com/2001/COMMUNITY/10/30/Schwartz/index.html.

108. *EFF Analysis of The Provisions of the USA Patriot Act*, *supra* note 18.

109. Rachel King & Lamar Smith, *Symposium: Q: Is Congress Giving Too Much Surveillance Power to Federal Law Enforcement?*, INSIGHT ON NEWS, Jan. 14, 2002, *at* http://www.insightmag.com/main.cfm/include/detail/storyid/160717.html (citing the affirmative response of Rachel King).

110. Interview with Ari Schwartz, *supra* note 107.

111. *See id.*

the warrant process of the courts.[112] Furthermore, these provisions are not limited to those suspected of terrorist activity, but to investigations of other crimes such as nonviolent tax violations or other offenses which do not pose the same threat of imminent harm to large numbers of people.[113]

The United States has already seen government authority abused in the past during wartime.[114] Before the USAPA, there was a restraint in government surveillance for FBI and foreign intelligence agencies because of previous misuse of surveillance powers, such as in 1974 when the FBI and foreign intelligence agencies spied on over 10,000 Americans, including Martin Luther King, Jr.[115] During World War II many innocent Japanese-Americans lost their civil liberties because of overreaching authorities.[116] The lesson learned in the past is that the American government works well with checks and balances.[117] The USAPA takes away protections built up over time rather than developing new and creative solutions.[118]

III. LEGAL TREATMENT

A. Defining Cable Broadband

Cable ISPs are unique because they provide both Internet and television services. Thus, they confront problems in complying with differing government regulations such as those that govern cable services in general (Cable Act),[119] those that govern the Internet (ECPA),[120] and those that govern both (USAPA).[121]

There is no one administrative agency, such as the FCC, that governs cable broadband.[122] One reason for this is that cable broadband has been

112. Rachel King & Lamar Smith, *Symposium: Q: Is Congress Giving Too Much Surveillance Power to Federal Law Enforcement?*, INSIGHT ON NEWS, Jan. 14, 2002, *at* http://www.insightmag.com/main.cfm/include/detail/storyid/160717.html (citing the affirmative response of Rachel King).

113. *Id.*

114. Interview with Ari Schwartz, *supra* note 107.

115. *EFF Analysis of The Provisions of the USA Patriot Act*, *supra* note 18.

116. Interview with Ari Schwartz, *supra* note 107.

117. *Id.*

118. *Id.*

119. *See* 47 U.S.C.S. § 551 (2001).

120. *See* 18 U.S.C.S. §§ 2701–2703 (2001).

121. *See* USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 224, 115 Stat. 272, 283–85, 295 (2001).

122. *See* Chen, *supra* note 28, at 681–82.

difficult to consistently define among courts and cable companies. Because of the various regulations cable ISPs have to comply with, cable ISPs and their subscribers, in turn, may be confused about their own regulation.

In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D)[123] demonstrates the difficulty in having different legislation govern cable broadband. In that case, government investigators requested that the District Court of the Southern District of New York order a cable company, Cablevision, to release one of its subscriber's personal information.[124] This information included the subscriber's name, home address, telephone number, social security number, driver's license number, billing information, and other identifying information.[125] Cablevision, argued that the Cable Act and the ECPA statutes required the cable company to act in conflicting manners.[126]

The court held that the Cable Act did not regard cable broadband as "cable service" because it defined the term as "(A) the one-way transmission to subscribers of (i) video programming, or (ii) other programming service, and (B) subscriber interaction, if any, which is required for the selection of such video programming or other programming service."[127] In other words, because Internet service does not involve the "one-way transmission" of service, cable broadband is not cable service.[128]

The circuit court in *AT&T v. City of Portland*[129] held that the Cable Act did not apply to cable broadband for similar reasons.[130] The *AT&T v. City of Portland* court specifically stated that Internet service was not "a 'cable service' as Congress defined it in the [Cable] Act."[131]

Contrary to *AT&T v. City of Portland*, the court in *MediaOne Group, Inc. v. County of Henrico*[132] held that cable modem services fell under the

123. 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001). The USAPA amended this conflict.

124. *Id.* at 287.

125. *Id.* at 288.

126. *Id.*

127. 47 U.S.C. § 522(6) (1994).

128. *In re Application of the United States*, 157 F. Supp. 2d at 290. *Contra* MediaOne Group, Inc. v. County of Henrico, 257 F.3d 356 (4th Cir. 2001).

129. 216 F.3d 871 (9th Cir. 2000).

130. *See id.* at 877.

131. *Id.* at 876; *see also* 47 U.S.C. § 522(6). The court used the term "Communications Act" to refer to the Communications Act of 1934 as amended by the Telecommunications Act of 1996. *Id.* Additionally, the Communications Act of 1934 had been amended by the Cable Act in 1984. *See CDT's Guide to Online Privacy*, Center for Democracy and Technology, *at* http://www.cdt.org/privacy/guide/protect/laws.html (last visited Jan. 15, 2002).

132. 97 F. Supp. 2d 712, 715 (E.D. Va. 2000) (finding that when a county ordinance conflicted with the Cable Act, the Cable Act prevailed), *aff'd* 157 F.3d 356 (4th Cir. 2001).

Cable Act's "cable" provision. Using Congress' definition of cable service as "the one-way transmission to subscribers . . . and . . . subscriber interaction,"[133] *MediaOne* held that because the cable service contains "news, commentary, games, and other proprietary content with which subscribers interact as well as Internet access, . . . it falls under the statutory definition of 'cable service.'"[134] Thus, the court argued that the cable-based Internet service fell squarely within the Cable Act's definition of "cable service."[135]

Moreover, the court concluded in *In re Application of the United States* that the cable company's Internet service fell within the Cable Act's "other service" provision.[136] In a 1992 amendment, Congress defined "other service" as "any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service."[137] This "other service" according to the court "plainly" includes cable modem service.[138]

Nevertheless, the *In re Application of the United States* court's findings are hardly indicative of much. *MediaOne* found that "the issue of the proper regulatory classification of cable modem service . . . is complex and subject to considerable debate."[139] The cable company in *In re Application of the United States* argued that "the scope of the Cable Act is a hotly-contested topic that is the subject of an ongoing proceeding before the FCC."[140] The court conceded that "courts have been loath to enter into the thicket of the general applicability of the Cable Act."[141] Thus, there is no clear answer of whether "cable service" includes cable Internet service or should have its own classification.[142] Despite this ambiguity with cable regulation in general, there is no doubt that cable ISPs fall under the

133. 47 U.S.C. § 522(6) (1994).

134. MediaOne Group, Inc. v. County of Henrico, 97 F. Supp. 2d 712, 715 (E.D. Va. 2000).

135. *Id.*

136. *In re Application of the United States*, 157 F. Supp. 2d at 291 (finding that "Congress did not intend that Internet service provided by a cable company be included within the requirements of subsection (h) [of 47 U.S.C. § 551]").

137. *In re Application of the United States*, 157 F. Supp. 2d at 291.

138. *Id.*

139. MediaOne Group, Inc. v. County of Henrico, 257 F.3d 356, 365 (4th Cir. 2001).

140. *In re Application of the United States*, 157 F. Supp. 2d at 290.

141. *Id.*; *see* United States v. Kennedy, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000) (declining to decide the scope of the Cable Act because the defendant in any case would not be entitled to suppression of the challenged evidence).

142. *See, e.g.*, *In re Application of the United States*, 157 F. Supp. 2d at 290; *Kennedy*, 81 F. Supp. 2d at 1111; MediaOne Group, Inc. v. County of Henrico, 257 F.3d 356, 365 (4th Cir. 2001).

ECPA's "electronic communications" regulations.[143]

B. A Lack of FCC Initiative

Another reason that cable ISPs have problems guaranteeing specific and consistent privacy protections is the lack of FCC initiative in regulating this area.[144] The lack of FCC regulation has left as many as forty million subscribers in an uncomfortable situation.[145] Without specific legislation in this area, cable companies will continue to struggle to simultaneously adhere to the Cable Act, the ECPA, and the USAPA.[146]

Because telephone lines were the first conventional means of going online,[147] one would think that the FCC regulated all Internet use. In fact, the court in *AT&T v. City of Portland* acknowledged that there "is a struggle for control over access to cable broadband technology,"[148] implying that regulation in this area was still up in the air. The court hinted that the FCC could regulate in this area but has failed to do so thus far.[149]

However, as cable television providers expand to provide Internet service, new questions arise as to regulation of these services.[150] The FCC generally regulates all ISPs and telecommunications.[151] Nevertheless, the FCC maintains a "hands-off" policy with respect to cable broadband,[152] while deciding to regulate only the less popular DSL high-speed Internet service.[153] However, the FCC should consider providing equal regulatory treatment of DSL and cable broadband.[154] The FCC declines to regulate cable broadband because it considers it an "information service"[155] rather than a "cable service"[156] or a "telecommunications service"[157] as defined by

143. 18 U.S.C. §§ 2701–2703 (1994).

144. Chen, *supra* note 28, at 681.

145. *Id.* at 682.

146. *See* discussion *supra* Part II (discussing the background of each Act).

147. *See* Medin & Rolls, *supra* note 16.

148. AT&T v. City of Portland, 216 F.3d 871, 873 (9th Cir. 2000).

149. *Id.* at 876.

150. *See* Chen, *supra* note 28, at 680. *See generally* Medin & Rolls, *supra* note 16.

151. *See* 47 U.S.C. § 153(43) (1994) (defining "telecommunications" as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received").

152. Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, 15 F.C.C.R. 19287, 19288 (2000).

153. *See* Chen, *supra* note 28, at 681; *MediaOne*, 257 F.3d at 363–64; 47 U.S.C. § 153(20).

154. Chen, *supra* note 28, at 713.

155. *Id.* at 680.

156. 47 U.S.C.S. § 522(6) (2001).

157. *Id.* § 153(46).

the Telecommunications Act of 1996. Despite the FCC's reluctance, at least one court has found that this definition of telecommunications applies to cable modem services.[158]

At present, no specific legislation governing cable broadband exists. Meanwhile, cable companies consider cable broadband as "cable" and "electronic communications" governed by various federal regulations.[159] Some other cable companies, including Cablevision, contend that cable broadband is neither a cable service nor a telecommunications service, for regulatory purposes.[160] Whatever the case, the lack of legislation governing cable broadband forces the providers and courts to rely on existing Internet, cable, and telecommunications legislation for regulation.[161]

There are times when the FCC has sought to regulate cable broadband and cable television service. In *National Cable & Telecommunications v. Gulf Power Co.*,[162] the Court found the FCC had authority under the Pole Attachments Act to regulate the rates, terms, and conditions for attachments to telephone and electric poles of wires providing commingled (i.e., Internet access and television service) services.[163] The Supreme Court in *National Cable* held that the FCC had authority to regulate rent paid by cable and telecommunications services providers for attachment of wires to power companies' poles, although the attachments were not solely used for cable service or telecommunications services.[164] However, there are times where courts will intervene by striking down the application of the FCC's use of federal legislation on cable.[165]

In addition, section 222 of the 1996 Telecommunications Act[166] governs the privacy of customer information and the regulation of the Internet where accessed over DSL or standard telephone lines.[167] A minor

158. *MediaOne*, 257 F.3d at 365.

159. *See In re Application of the United States*, 157 F. Supp. 2d at 289.

160. *See* Nat'l Cable & Telecomm. Assoc., Inc. v. Gulf Power Co., 2002 U.S. LEXIS 491, at *12, *23 (2002).

161. *See generally* Chen, *supra* note 28, at 683–84; *In re Application of the United States*, 157 F. Supp. 2d at 287.

162. 2002 U.S. LEXIS 491, at *8–*9 (2002).

163. *Id.* at *8, *16.

164. *Id.* at *17.

165. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1228 (10th Cir. 1999).

166. 47 U.S.C. § 222 (1994) (amending the Communications Act of 1934).

167. *See generally* 47 U.S.C.S. § 157 (2001); Rachel V. Abramson and Amy C. McMenamin, Keeping the Toddler out of the Cookie Jar: An Overview of Internet Website and Communications Privacy Issues 13 (Nov. 2000), *available at* http://www.l-Olaw.com/Publications/cookietoc.book.pdf (white paper developed for Lampert & O'Connor, P.C.).

debate exists as to its application to cable broadband. Until the introduction of cable broadband, section 222 of the Telecommunications Act determined the regulations of Internet user's privacy.[168] Section 222 regulated the disclosure of Customer Proprietary Network Information ("CPNI"), which is "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to" by any of its customers.[169] Section 222 protects information about the subscriber's services, including the length, place, and costs of calls that a subscriber makes.[170] The disclosure of such information is subject to consent by the subscriber, unless the subscriber's use of the service is unlawful, fraudulent, abusive, or for purposes of creating a directory.[171]

Congress has advised that section 222 on privacy restrictions of the Telecommunications Act was not applicable to Internet use.[172] According to Congress, the Internet was not a "telecommunication service," but an "information service" under the Telecommunications Act's definitions. Thus, section 222 did not apply to ISPs.[173] Section 222 is applicable only to "telecommunication" providers.[174] However, there is legal argument that cable broadband could fall under the Telecommunications Act as an "advanced telecommunications capability."[175] The telecommunications provisions of the Federal Communications Act define "advanced telecommunications capability" as any "high speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology," which could possibly include cable broadband.[176] This definition is not applied broadly nor is there a clear indication that the

168. H.R. CONF. REP. NO. 104-458, at 205 (1996) ("[I]n general, the new section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI. New subsection 22(a) stipulates that it is the duty of every telecommunications carrier to protect the confidentiality of proprietary information of and relating . . . customers.").

169. 47 U.S.C. § 222(h) (1994).

170. *See id.* § 222(c).

171. *Id.* §§ 222(c)–(d).

172. *See generally* JASON OXMAN, THE FCC AND THE UNREGULATION OF THE INTERNET 18 (Office of Plans and Policy, Working Paper No. 31, July 1999), *available at* http://www.fcc.gov/Bureaus/OPP/ working-papers/oppwp31.pdf.

173. *See id.* (reporting that basic service, referred to as "telecommunications services," and enhanced services, referred to as "information services," were separate and distinct categories of service).

174. *See id.*

175. Telecommunications Act, Pub. L. No. 104-104, § 706, 110 Stat. 56, 153 (1996) (amending the Federal Communications Act).

176. *Id.*

Telecommunications Act regulates this area.[177]

Because the Internet was originally accessed by telephone lines, the FCC could apply section 222 of the Telecommunications Act to the Internet.[178] However, with the advent of cable broadband, the FCC decided that Internet services were not telecommunications services.[179] This year the FCC declined to decide whether Internet services are cable services.[180] The FCC did pledge in 1999 to continue to monitor broadband developments closely to see its effects on its goal of encouraging deployment of broadband capabilities.[181] However, it appears that FCC initiative in the cable broadband area has decreased. In *Telecommunications, Inc.*,[182] the FCC missed its chance to seize the regulatory initiative by declining to impose certain open access rules as a condition for the approval of AT&T's acquisition of TCI (a cable company).[183] Instead, the FCC proposed a formal proceeding to clarify the commission's role in creating a national broadband policy and announced that it would reexamine its approach to cable broadband.[184] Currently, the FCC is contemplating establishing a classification for cable broadband.[185] As Justice Thomas said in his dissent in *National Cable*, "[s]uch a determination would require the Commission to decide at long last whether high-speech Internet access provided through cable wires constitutes cable service or telecommunications service or falls into neither category."[186]

The issue of whether cable broadband is regulated by cable or telecom rules is currently pending before the FCC.[187] There are a number of regulatory approaches possible; the FCC must decide whether or not to treat cable broadband as a "cable service," a "telecommunications service,"

---

177. David R. Goodfriend, *Cable Television Privacy Requirements Enter the World of Internet Service Providers*, 5 N.Y.L. SCH. MEDIA LAW & POL'Y 1, 3–4 (1997).

178. 47 U.S.C.S. § 222 (2001).

179. *Nat'l Cable*, 2002 U.S. LEXIS 491, at *18. The FCC has suggested a willingness to reconsider its conclusion that Internet services are not telecommunications. *Id.* at *20.

180. *Id.*

181. Chen, *supra* note 28, at 683.

182. *See* 14 F.C.C.R. 3160 (1999).

183. *Id.* at 3192, 3207.

184. Chen, *supra* note 28, at 683.

185. *2001 Annual Report*, A.B.A. SEC. OF PUB. UTIL., COMM., AND TRANSP. LAW 111.

186. *Nat'l Cable*, 2002 U.S. LEXIS 491, at *35. Justice Thomas dissented stating that the lack of FCC's decisiveness hampered the Court's ability to review the Commission's order in a logical manner. *Id.* at *40. "Judicial review of [an agency's] orders will . . . function accurately and efficaciously only if the [agency] indicates fully and carefully the methods by which . . . it has chosen to act. *Id.* at *41. Here, the FCC obviously has fallen far short of this standard." *Id.* at *40–*41.

187. *Cable Notes*, WARREN'S CABLE REG. MONITOR, Sept. 3, 2001, 2001 WL 8146810.

an "information service," or an entirely hybrid service subject to multiple provisions.[188] According to Justice Thomas, the FCC's attempt to regulate the Internet in some areas, such a rates for attachments, while refusing to classify the services is "arbitrary, capricious," and "not in accordance with the law."[189] Hence, the regulation of cable-based access to the Internet has become one of the most controversial subjects in communications law.[190]

IV. CABLE BROADBAND SUBSCRIBERS' RECORDS HAVE BECOME A GOVERNMENT DATABASE

The current state of regulation for cable broadband subscribers poses civil liberty concerns because of diminished privacy protection.[191] Specifically, the USAPA amends past anomalies, but goes too far by giving too much power to federal investigators for Internet-related searches.[192] In other words, Congress had the right intentions, but acted on them in the wrong way. The irony is that President Bush called the USAPA "an essential step in defeating terrorism, while protecting the constitutional rights of all Americans."[193] This Part discusses three new privacy regulations affecting cable broadband subscribers.

A. Reduction of Privacy for Cable Records

Section 211 of the USAPA, entitled "Clarification of Scope," amends the previous statutory conflict between the Cable Act and the ECPA.[194] President Bush recognized that the USAPA amended laws that became unclear with the advent of new technology, such as cable broadband.[195] He stated, "As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology."[196]

---

188. *See* Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, 15 F.C.C.R. 19287, 19293 (2000).

189. *Nat'l Cable*, 2002 U.S. LEXIS 491, at *42.

190. *See* Chen, *supra* note 28, at 680.

191. *See* USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 224, 115 Stat. 272, 283–85, 295 (2001).

192. *See id.*

193. *Bush Comments on Signing New Antiterrorism Law*, *supra* note 98.

194. USA Patriot Act § 211.

195. *See Bush Comments on Signing New Antiterrorism Law*, *supra* note 98 ("The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones.").

196. *Id.*

Prior to the USAPA, *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D)*[197] demonstrated how a cable ISP had to comply with conflicting federal regulations. The cable ISP was concerned with civil liabilities and not adhering to privacy promises afforded to general cable subscribers.[198] The Cable Act afforded notice and the opportunity to contest any order to disclose personal information to the government.[199] Nevertheless, the court denied the motion to quash disclosure of personal information.[200] This case of first impression highlighted the surprising privacy protections afforded cable Internet users under the Cable Act[201] and the ECPA.[202]

The USAPA resolves the statutory conflict between the ECPA and the Cable Act.[203] The previous law contained two regulations regarding privacy protection of communications and their disclosure to law enforcement—one governing cable service (the Cable Act) and the other applying to the use of telephone service and Internet access (the ECPA).[204] Prior to the amendments, the Cable Act provided more restrictive rules governing law enforcement access to most of the records possessed by the cable company.[205] For instance, the Cable Act did not allow the use of subpoenas or search warrants to obtain such records. Instead, the cable company had to provide notice to any customer, including those who were targets of criminal investigations.[206] The government also had to justify to a court the investigative need for the records, while allowing the customer to appear in court with an attorney to contest the order.[207] The government had to prove there was clear and convincing evidence that there was reasonable suspicion that the subject of the information was engaging in criminal activity and that the information sought would be material evidence in the case.[208] Using the court's discretion, the court could order a

197. 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001).

198. *See id.* at 288–89.

199. *See id.*

200. *See id.* at 292.

201. 47 U.S.C. § 551 (1994), *amended by* USA Patriot Act, Pub. L. No. 107-56, § 211, 115 Stat. 272, 283 (2001).

202. 18 U.S.C. §§ 2701–2703 (1994), *amended by* USA Patriot Act §§ 209–210, 212, 224.

203. *See* USA Patriot Act §§ 210–212.

204. *See* U.S. DEP'T OF JUSTICE, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001, §§ 209–212 (2001), *at* http://usdoj.gov/criminal/cybercrime/PatriotAct.htm. (last visited Nov. 10, 2001) [hereinafter FIELD GUIDANCE].

205. *Id.*

206. 47 U.S.C. § 551 (1994).

207. FIELD GUIDANCE, *supra* note 204.

208. 47 U.S.C. § 551(h) (1994), *amended by* USA Patriot Act § 211.

disclosure of the records.[209]

Because of the requirements stated above, governmental entities found this procedure "completely unworkable" for criminal investigations.[210] Giving notice to subscribers, granting hearings for rebuttal, or waiting for approvals of warrants or court orders not only took time, but also provided hints to the criminal suspect that the government was investigating him or her.[211] These complications delayed or ended important investigations.[212] Thus, the USAPA eliminated treating identical records differently depending on the technology used to connect to the Internet.[213] Instead of the Cable Act governing the disclosure of Internet subscriber's information to the government, the ECPA provisions prevail.[214]

The USAPA's amendment to the Cable Act, allowing disclosure of information to a government entity without any notice or hearing,[215] may also affect cable television subscriber's privacy rights as well. The Cable Act still protects records revealing what ordinary cable television programming a customer chooses to purchase.[216] For instance, particular premium channels or pay-per-view shows are not disclosed to the government.[217] However, with the amendment to the Cable Act, cable television subscribers' right to notice and a hearing for court-ordered information may not be useful anymore.[218]

As federal investigators of cable television subscribers have more options in obtaining subscriber information, they no longer are limited to seeking a court order pursuant to section 551(h) for disclosure of information.[219] These federal investigators can essentially skip the delays of providing notice and a hearing to obtain personal subscriber information under section 551(h) by seeking information under a subpoena, pursuant to section 551(c)(2)(D).[220] Therefore, USAPA renders the requirement of a hearing and notice for disclosure pursuant to a government order for Internet users and arguably, cable television users, practically useless.

---

209. *See* FIELD GUIDANCE, *supra* note 204.
210. *Id.*
211. *See id.*
212. *Id.*
213. *See id.*
214. *Id.*
215. 47 U.S.C.S. § 551(c)(2)(D) (2001).
216. FIELD GUIDANCE, *supra* note 204.
217. *Id.*
218. *See generally* 47 U.S.C.S. § 551.
219. *Id.*
220. *Id.*

In conclusion, the ECPA, the wiretap statute and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services, such as telephone and Internet services.[221] The USAPA eliminates hindrances to federal investigations of the prior regulations imposed and clarifies the scope of the Cable Act. These are significant accomplishments, but the Act goes too far in allowing unchecked government access to Internet user's personal information.

B. Expanded Use of Subpoena

In section 210 of the USAPA, entitled "Scope of Subpoenas for Electronic Evidence," Congress expanded the records the government may seek with a subpoena to include records of session times and durations, temporarily assigned network (IP) addresses, and means and source of payments, which include credit card or bank account numbers.[222] Before the amendment, the information obtained through a subpoena was limited to information such as the customer's name, address, and length of service.[223] In fact, critics had previously criticized the ECPA as allowing the FBI and other agencies to too easily obtain customer records.[224] Now, the current provision allows the government to subpoena information relevant to determining a customer's true identity.[225] Obtaining the method of payment allows an easier determination of a customer's true identity.[226] Thus, in effect, investigators may identify Internet subscribers who decided to register for service under false names. This helps hold individuals responsible for criminal acts committed online.[227]

In addition, the ECPA provisions, prior to the amendments, were technology-specific and related primarily to telephone communications.[228] With the amendments, the ECPA not only provides for "local and long distance telephone toll billing records" but now includes "records of session times and durations" too.[229] Furthermore, language added included

221. *See* FIELD GUIDANCE, *supra* note 204. The wiretap statute, 18 U.S.C. §§ 2510–2522 (2000), and the trap and trace statute, 18 U.S.C. §§ 3121–3127 (2000), are beyond the scope of this Comment.

222. *Id.*

223. *Id.* This information includes start date of service, type of services utilized, telephone number, and subscriber number or other identifying number. 18 U.S.C. § 2703(c) (1994).

224. *Electronic Communications Privacy Act*, *supra* note 69 (criticizing procedures as easily rationalized because no judicial review was required).

225. *See* FIELD GUIDANCE, *supra* note 204.

226. *See id.*

227. *See generally id.*

228. *Id.*

229. *Id.*

the IP address assigned by the provider to the customer for a particular session, and the remote IP address from which a customer connects to the provider.[230]

Lastly, the USAPA allows for subpoenas of electronic records nationwide. Previously, subpoenas were limited to the geographic jurisdiction of the court approving the surveillance.[231]

These expansions are problematic because certain information is readily available to any governmental entity through a subpoena.[232] A subpoena is not an obstacle to the government because there is no court review required for a subpoena.[233] A better system of checks and balances would require a judge to review actual evidence and determine if there is probable cause for investigating a suspect. In addition, oversight records should be kept to ensure that government power is not abused.[234]

Furthermore, the court in *Parker v. Time Warner Entertainment Co.*[235] examined the legislative history of the ECPA, finding impermissible disclosure to third parties of the extent to which a subscriber viewed a particular service (including when and how long the subscriber used the service). Disclosure was limited to the name, address, and the type of services[236] the subscriber had purchased.[237] Although *Parker* addressed cable television service, the USAPA contradicts *Parker*'s interpretation of the legislative history of the ECPA.[238] The USAPA provides no similar limitation on disclosures.[239]

Moreover, expansion of the subpoena has greater consequences than realized.[240] The feature of anonymity on the Internet is no longer the same. Now that the government can obtain personal identifying information easily, society is one step closer to a "Big Brother" environment. In essence, the USAPA grants "the FBI broad access to sensitive business

230. *Id.*

231. *See Changes Being Considered by Congress*, American Civil Liberties Union, *at* http://www.aclu.org/congress/patriot_chart.html (Oct. 10, 2001).

232. *See* FIELD GUIDANCE, *supra* note 204; *EFF Analysis of The Provisions of the USA Patriot Act*, *supra* note 18; *In re Application of the United States*, 157 F. Supp. 2d at 288.

233. *See* FIELD GUIDANCE, *supra* note 204.

234. Interview with Ari Schwartz, *supra* note 107.

235. No. 98CV4265(ERK), 1999 WL 1132463, at *9 (E.D.N.Y. Nov. 8, 1999).

236. "Type of service" refers to the subscriber's access to specific packages or channels. *See id.*

237. *Id.*

238. *See* USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 115 Stat. 272, 283–85 (2001) (enacting amendments to the Electronic Communications Privacy Act).

239. *See* FIELD GUIDANCE, *supra* note 204.

240. *See Changes Being Considered by Congress*, *supra* note 231.

records about individuals without having to show evidence of a crime."[241]

C. Voluntary Disclosures

In section 212 of the USAPA, entitled Emergency Disclosures by Communication Providers, ISPs are now able to voluntarily disclose all "non-content" customer information to law enforcement without a court order or subpoena.[242] This provision sunsets December 31, 2005,[243] meaning that the legislation will expire unless Congress renews it before the deadline.[244] Prior to the USAPA, no special provisions allowed ISPs to disclose customer records or communications, even in emergencies involving immediate risk of death or serious physical injury to any person.[245] Under prior law, if an ISP disclosed such records or communication it potentially faced civil liability.[246]

Section 212 also corrects an anomaly in the current law by permitting a provider to disclose non-content records (such as subscriber's log-in records) as well as the contents of the customer's communications to protect their computer systems.[247] For purposes of the ISP's self-protection, the ECPA, prior to the USAPA, did not allow disclosure of non-content information to law enforcement, but did allow disclosure of content-information.[248] This amendment was appropriate given the right to disclose the content of communications necessarily implied the less intrusive ability to disclose non-content records.[249]

This provision of the USAPA is an adequate measure to handling terrorism. The provision actually addresses the purpose of the USAPA—to combat terrorism.[250] For example, if an ISP independently learned that a customer was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the customer's account information to law enforcement could potentially save lives.[251] Congress also provided that this provision will sunset in 2005,[252] which appropriately ensures a check

241. *USA Patriot Act Boosts Government Powers*, *supra* note 103.
242. FIELD GUIDANCE, *supra* note 204.
243. *Id.*
244. *See id.*
245. *Id.*
246. *Id.*
247. *Id.*
248. FIELD GUIDANCE, *supra* note 204.
249. *Id.*
250. *See generally id.*
251. *Id.*
252. *Id.*

on this new power. Furthermore, this voluntary disclosure provision "does not create an affirmative obligation" of ISPs to review customer communications "in search of such imminent dangers."[253]

V. BALANCE BETWEEN PRIVACY AND SECURITY

A. Privacy Versus Security

Is the cost of privacy outweighed by the need for criminal justice? Should the government put the privacy of millions of innocent Internet users at risk to monitor only a guilty few?[254] With growing reliance on the Internet as a tool for communication, research, pleasure, and business,[255] the information superhighway needs some protection for its users. Online privacy is desired because people want their activities and personal information to be safe online.[256] Moreover, the sense of anonymity is an online feature.[257] Accordingly, ISPs want to maintain privacy for their consumers.[258] ISPs understand that addressing their subscriber's Internet privacy concerns will help them expand the use of the Internet.[259] Currently sixty percent of Americans say security and privacy worries keep them from doing business online.[260] Thus, ISPs and other online service providers want to preserve protections to encourage the U.S. Internet economy and market.[261]

However, Americans desire security from crime, especially since the attacks on September 11, 2001. "[T]errorist attacks have prompted a few Americans to say they are more willing to trade some personal privacy for security. . . ."[262] A *Washington Post* poll revealed two in three Americans

253. *Id.*

254. *Privacy in America: Computers, Phones & Privacy*, American Civil Liberties Union, *at* http://www.aclu.org/library/ibpriv3.html (last visited Nov. 13, 2001).

255. *See Privacy Rights—Introduction*, American Civil Liberties Union, *at* http://www.aclu.org/issues/privacy/isprivacy.html (last visited Nov. 13, 2001).

256. *See id.*

257. *See Privacy in America: Computers, Phones & Privacy*, American Civil Liberties Union, *at* http://www.aclu.org/library/ibpriv3.html (last visited Nov. 13, 2001).

258. *See generally In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D), 157 F. Supp. 2d 286, 288–290 (S.D.N.Y. 2001).

259. *See* Jeff Sweat, *Privacy—Can Businesses Build Trust and Exploit Opportunity?*, INFORMATIONWEEK, Aug. 20, 2001, at 30.

260. *Id.* at 31.

261. *See id.* at 30.

262. Bartlett, *supra* note 11 (commenting on a study by Pew Research Center on the state of civil liberties one week after the September 11, 2001 terrorist attacks on the United States).

were willing to surrender some liberties to crack down on terrorism.[263] In a similar poll by the Pew Research Center, seventy percent of Americans generally support the concept of sacrificing some civil liberties in order to curb terrorism.[264] However, in a 1997 Pew Research center study, before the attacks, only twenty-nine percent of Americans would sacrifice civil liberties to curb terrorism.[265] Should the actions of one terrorist group dramatically change how Americans value their Bill of Rights? Conversely, prior to September 11, did Americans overvalue privacy over security?

In an example of curbing liberties for security procedures, it appears federal investigators started wiretapping telephone lines hours after the first attack.[266] The apparent wiretapping resulted in some arrests after investigators heard suspects praise the terrorist attacks.[267] Thus, the government maintained security through its ability to act swiftly in a criminal investigation.[268]

Similarly, the president of the American ISP Association spoke on ISP compliance with government security procedures: "As always, when the government meets the established burden of proof, then the Internet service provider supplies the data. The ISP is not above the law."[269] The latter statement is true in that ISPs should comply with government security measures when necessary. However, establishing reasonable requirements for obtaining the data is essential in protecting the subscriber's personal information.

Because the Internet is such a powerful information tool, it demands more careful privacy protection. Danger exists because the Internet provides access to so much information. People's identities and personal information are subject to disclosure to the wrong parties and misuse by the government.[270] The United States government has previously used its intelligence gathering and sharing abilities among agencies to disrupt

263. Nat Hentoff, *Liberty Is A Fragile Thing*, VILLAGE VOICE (Sept. 19–25, 2001), *at* http://villagevoice.com/issues/0138/hentoff.php (citing a *Washington Post* poll).

264. Bartlett, *supra* note 11.

265. *Id.*

266. *See* Interview with Ari Schwartz, *supra* note 107.

267. *See id.*

268. *See generally id.*

269. Patrick Ross, *Terrorist Attacks Shift Internet Debate from Privacy to Security*, WASH. INTERNET DAILY, Sept. 20, 2001, LEXIS, Newsletter Stories (quoting Sue Ashdown, president of the American ISP Association).

270. *See* Senator Patrick Leahy, Statement of Senator Patrick Leahy, Chairman, Senate Judiciary Committee, and Democratic Manager of the Senate Debate on the Anti-Terrorism Bill (Oct. 25, 2001), *at* http//www.senate.gov/~leahy/press/200110/102501.html.

domestic groups and lawful activist groups, including environmental groups, women's liberation activists, and other organizations that have mounted peaceful protests.[271] Similarly, the USAPA allows broad monitoring of all Americans because Congress did not narrowly tailor the statute to monitor only terrorists.[272]

A great deal of information is available from an ISP about its Internet users' online activities.[273] Customers trust ISPs with credit card information, social security numbers, driver's license numbers, and other personal identification information. ISPs maintain that trust by providing privacy statements to subscribers and a medium to conduct everyday personal and private activities online.[274] Thus, ISPs must not disclose more than legally required because of the huge costs involved—violations of customers' privacy and trust.

There is an inherent protection of privacy in the Fourth Amendment of the Constitution, which protects individuals against illegal searches and seizures.[275]

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[276]

The Fourth Amendment triggers restrictions when the government invades one's privacy, even if there is no actual intrusion or invasion into protected space.[277] The Fourth Amendment protects people and not simply areas against unreasonable searches.[278] This means that, to a certain extent, individuals receive protection from governmental intrusion.[279] If, out of

---

271. *Id.*

272. *See* USA Patriot Act, Pub. L. No. 107-56, §§ 209–212, 115 Stat. 272, 283–85 (2001).

273. *See Privacy Rights—Introduction*, American Civil Liberties Union, *at* http://www.aclu.org/issues/privacy/isprivacy.html (last visited Nov. 13, 2001).

274. *See CDT's Guide to Online Privacy*, *supra* note 49; *see also Privacy Rights—Introduction*, American Civil Liberties Union, *at* http://www.aclu.org/issues/privacy/isprivacy.html (last visited Nov. 13, 2001).

275. U.S. CONST. amend. IV.

276. *Id.*

277. *See id.*

278. *See id.*

279. *CDT's Guide To Online Privacy*, *supra* note 49. Under the Privacy Protection Act of 1980 ("PPA"), Congress restricted law enforcement searches and seizures on publishers, those who "have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." *Id.* The PPA forces law enforcement to use subpoenas or voluntary cooperation for searches and seizures, when there is probable cause to believe the

fear, Americans start allowing the government to search and seize their personal online information without notice, they may witness the slow degradation of their constitutional privacy rights.

Additionally, notice to the suspect provides a person an opportunity to assert his Fourth Amendment rights.[280] For instance, a person can correct an officer of the law if he is searching the wrong address or can question the officer for looking in an area not specified in the warrant.[281] The Right to Financial Privacy Act is another federal act that requires notice to a party regarding disclosure of certain information, but the USAPA overrides this act and denies notice to the party.[282] Although the government's ability to access pertinent information is important in reducing crime, there is no reason why a subscriber should not have notice of a "search" of his personal information.

As cable companies' privacy statements may seem to provide some sense of privacy protections, users probably presume that there will be notification of disclosure of personal information to third parties. As a result of the USAPA, these privacy statements, usually vague in and of themselves, may misinform subscribers of their rights and expectations. For example, a cable television and Internet subscriber may not understand that the government can obtain certain personal information through their Internet account, but not through their television account.[283] Under the ECPA, the governmental entity would compel the ISP to disclose only those customer records relating to Internet service.[284] However, television subscribers still have a right to appear and contest any criminal investigation pursuant to a court order before the cable company discloses their personal information, even though the USAPA has limited the likelihood of this.[285]

---

publisher has committed or is committing a criminal offense to which the materials relate. *See id.* Arguably, the PPA extends to computer bulletin boards and on-line systems under the "other form of public communication" clause of the Act, but no case law has concluded this assertion. *See id. See generally* Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (1994).

280. Rachel King & Lamar Smith, *Symposium: Q: Is Congress Giving Too Much Surveillance Power to Federal Law Enforcement?*, INSIGHT ON NEWS, Jan. 14, 2002, *at* http://www.insightmag.com/main.cfm/include/detail/storyid/160717.html (citing the affirmative response of Rachel King).

281. *Id.*

282. *Id. See generally* Right to Financial Privacy Act, 12 U.S.C.S. §§ 3401–3412 (2001). Delayed notification also prevents timely judicial review of searches because pending investigations can last many years. Lincenberg & Gluck, *supra* note 105.

283. *See* FIELD GUIDANCE, *supra* note 204.

284. *See id.*

285. *See generally id.*; *In re* Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D), 157 F. Supp. 2d 286 (S.D.N.Y. 2001).

In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(D)[286] demonstrates how much the government can obtain through a court order given the cable ISP was ordered to disclose the subscriber's name, home address, email address, telephone number, social security number, driver's license number, billing information, and other identifying information. The court order also required disclosure of any accounts opened by the subscriber, hardware installed on the subscriber's computer to establish the computer cable connection, any "Optimum internet provider addresses" used by the subscriber (including connection and disconnection times), the method of connection, the amount of data transferred to the subscriber's account, and other information pertaining to the Internet provider address.[287] Lastly, the order directed the cable ISP not to disclose the existence of the investigation to the listed subscriber or any other person, until otherwise ordered by the court.[288] All of this information disclosure was appropriate under the ECPA.[289]

What is even more disconcerting is that sanctions against government surveillance misuses are weak.[290] If the government partakes in an illegal search and seizure, the exclusionary rule will operate to exclude highly relevant and powerful evidence in court.[291] However, the exclusionary rule suffers from shortcomings.[292] Several exceptions exist that allow admission of evidence, and judges are often reluctant to exclude highly valuable evidence based on a technical violation of a warrant.[293] In addition, exclusion is not an available sanction for evidence used outside the court.[294] Thus, abusive surveillance can continue as an information-gathering tool that can lead law enforcement to admissible evidence.[295]

Another sanction for violation of the fourth amendment is the infrequently used mechanism of seeking civil and criminal sanctions against agents.[296] These are usually unsuccessful because it is difficult to find out about illegal surveillance and to recover damages for

286. 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001).

287. *Id.*

288. *Id.*

289. *See generally* 18 U.S.C. § 2703 (1994) (listing the type of information that may be disclosed by a governmental entity).

290. *See* Young, *supra* note 49, at 1073–78.

291. *Id.* at 1074.

292. *Id.*

293. *Id.* at 1075.

294. *Id.* at 1076.

295. *Id.*

296. Young, *supra* note 49, at 1078.

infringement.[297] First, learning about illegal surveillance with sufficient certainty to warrant litigation is difficult.[298] Second, obtaining this information under the Freedom of Information Act is usually defeated by executive privilege.[299] Third, the president obtains absolute immunity against damages, while other executives are also immune.[300] Fourth, the case is often not justiciable.[301] In addition, police officers can claim the common-law defense of good faith, while federal officers can claim qualified immunity.[302]

What is the right balance? President Bush and legislative leaders called the USAPA a bill that strikes "just the right balance between security concerns arising out of recent terrorist attacks and the protection of traditional civil liberties . . . ."[303] At the same time, critics argued that the USAPA was "dangerous legislation" with "too many weaknesses in the bill that could end up curbing and infringing fundamental civil rights and liberties . . . ."[304] The broad sweeping USAPA provides changes in the laws that are inexpedient to combat terrorism. As it takes a great amount of time to think about all the possible unintended consequences of the legislative language, Congress should have taken the time to think about the consequences of the new amendments on required disclosures of Internet subscribers' information.[305]

B. Future Ramifications of Reduced Online Privacy

As the use of the Internet expands, the decrease in privacy protections might be something Congress regrets. During wartime, "electronic privacy [has] suddenly seemed like a needless luxury."[306] For example, the information-sharing authorizations under the USAPA allow the CIA greater abilities to spy on Americans.[307] One critic stated, "Once the CIA makes clear the kind of information it seeks, law enforcement agencies can

297. *Id.*

298. *Id.*

299. *Id.*

300. *Id.*

301. *See id.*

302. Young, *supra* note 49, at 1078.

303. *Bush Comments on Signing New Antiterrorism Law*, *supra* note 98.

304. *The Response to Terror: Bush Signs Antiterrorism Bill*, ASIAN WALL STREET J., Oct. 29, 2001, at 7 (quoting Ralph Neas, president of the liberal People for the American Way).

305. *See Changes Being Considered by Congress*, American Civil Liberties Union, *at* http://www.aclu.org/congress/patriot_chart.html (Oct. 10, 2001).

306. Brendan I. Koerner, *Technology and Its Discontents*, VILLAGE VOICE (Sept. 26, 2001), *at* http://villagevoice.com/issues/0139/koerner.php.

307. *USA Patriot Act Boosts Government Powers*, *supra* note 103.

use tools like wiretaps and intelligence searches to provide data to the CIA."[308] This runs counter to the National Security Act of 1947, which draws a sharp line between foreign intelligence and law enforcement by stating that the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions."[309]

Similarly, it is troubling that the drafters of the USAPA may have left open questions about whether the Cable Act, the ECPA, and the USAPA apply to future developments in technology. For instance, the ECPA privacy provisions for governmental access now cover all "wire and electronic communications," instead of just "electronic communications."[310] This blanket definition arguably covers a broad range of communication devices developed in the future.

Allowing the government broad and flexible powers to regulate, monitor, and obtain personal information can result in a slippery slope problem. Now, various governmental entities can easily share expanded information through a subpoena and "content" communications through a warrant or court order.

An example of the slippery slope problem is the government's misuse of social security numbers. First, when signing up for cable television service or cable broadband, companies require the subscriber's social security number.[311] Under the Privacy Act of 1974,[312] federal law requires federal, state, and local government agencies to provide a "disclosure" statement to its customers explaining why they might require a social security number.[313] Even if providing social security numbers upon request is optional, the agencies still need an explanation of such request.[314] Although Congress designed the Privacy Act of 1974 "to protect individuals from an increasingly powerful and potentially intrusive federal government,"[315] the government can still obtain this information from cable ISPs through a loophole of the Privacy Act 1974.[316]

---

308. *Id.*

309. 50 U.S.C.S § 403-3 (2001); *see also* Senator Patrick Leahy, Statement of Senator Patrick Leahy, Chairman, Senate Judiciary Committee, and Democratic Manager of the Senate Debate on the Anti-Terrorism Bill (Oct. 25, 2001), *at* http//www.senate.gov/~leahy/press/200110/102501.html.

310. *See* FIELD GUIDANCE, *supra* note 204.

311. *See* Bill Olds, *No Way to Stop the Spread of Social Security Numbers*, HARTFORD COURANT, Aug. 26, 2001, at H3, 2001 WL 25319587.

312. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974).

313. Olds, *supra* note 311.

314. *Id.*

315. *CDT's Guide to Online Privacy*, *supra* note 49.

316. *See generally id.* (explaining that the prohibition, under the Privacy Protection Act of

The government should not need one's social security number for a federal investigation in the first place. The federal government created the system of social security numbers exclusively to monitor earnings to determine the amount of tax liability of each worker.[317] The uses of social security numbers today has drifted far from the government's original purpose.[318] For example, credit bureaus manage 400 million files that reveal information keyed to around ninety percent of the American adult public.[319] Selling and trading this information is subject to minimum legal limitations.[320] Banks, insurance companies, and others that have major financial influence do not want limitations in this area, which is why Congress is reluctant to restrict use of social security numbers.[321]

Notably, some state legislatures have passed limitations on the use of social security numbers by government agencies.[322] Continuing this trend will stop the slippery slope problem that has arisen in the use of social security numbers. The government's use of social security numbers should be limited to its original purpose—the collection of taxes.[323] In turn, the corporate and business exploitation of social security numbers should be limited, too.[324] Therefore, an individual's social security number should not be subject to government disclosure.

Finally, the USAPA aims to combat terrorists, not the entire country. President Bush believes the new law "will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones."[325] However, "the government has not shown that its previous powers to conduct surveillance or to prosecute computer crime were a significant barrier to investigating or preventing terrorist attacks."[326] If investigators really did need these new powers, Congress should have at

---

1974, against disclosing records to third parties is weakened by several exceptions).

317. Olds, *supra* note 311.

318. *See id.*

319. *Id.*

320. *Id.*

321. *Id.*

322. In Connecticut, registrars of voters convinced the state legislature to eliminate a procedure of collecting social security numbers during voter registration and providing them to a private contractor to compile lists of randomly selected persons to serve on state court juries. *Id.* However, the jury administrator now collects the social security numbers through different state agency lists, such as motor vehicle lists, tax department lists, and labor department lists. *Id.*

323. Olds, *supra* note 311.

324. *See id.*

325. *Bush Comments on Signing New Antiterrorism Law*, *supra* note 98.

326. *EFF Releases Analysis of USA-Patriot Act (USAPA)*, EFFECTOR ONLINE NEWSLETTER (Electronic Frontier Foundation), Oct. 25, 2001, *at* http://www.eff.org/effector/HTML/effect14.34.html.

least incorporated judicial oversight in certain measures to ensure no abuses occur.[327] This judicial oversight is lacking in the USAPA. The effect of the USAPA will harm American society, by breaking down U.S. constitutional privileges and guarantees. The provisions discussed in this Comment do not specifically target fighting terrorism; rather, these provisions enhance general criminal investigation capabilities. In fact, the amendments at issue here merely combat nonviolent, domestic computer crime.[328] Although many of the provisions facially appear to be aimed at terrorism, there is no government showing that surveillance abilities at issue here would have been useful in curbing terrorism or detecting the planning of the September 11 attacks.[329]

Law enforcement should use these new powers carefully and limit their use to bona fide investigations into acts of terrorism.[330] If not, courts should punish those who misuse these powers and Congress should reexamine its decision to grant such broad powers.[331] Furthermore, "if these laws are misused to harm the rights of ordinary Americans involved in low level crimes unrelated to terrorism," courts should refuse to admit this evidence to prosecute them.[332]

VI. CONCLUSION

Congress appropriately addressed certain concerns regarding regulation of cable broadband through the USAPA. The USAPA addresses a pressing social concern over security and resolves statutory anomalies in the law. Yet there remains a need for reform in cable broadband privacy regulation as amended by the USAPA. This calls for further congressional action or even FCC initiative. A closer examination of the USAPA reveals that more appropriate legislative alternatives for curbing terrorism are available without compromising civil liberties. The USAPA threatens the "right to be let alone—the most comprehensive of the rights of man and the right most valued by civilized men."[333] Moreover, because the Internet is such a powerful information tool, it demands more careful privacy protection.

---

327. *Id.*

328. *EFF Analysis of the Provisions of the USA Patriot Act*, *supra* note 18.

329. *Id.*

330. *Id.*

331. *Id.*

332. *Id.*

333. *Privacy Rights—Introduction*, American Civil Liberties Union, *at* http://www.aclu.org/issues/privacy/isprivacy.html (last visited Nov. 13, 2001) (citing Justice Louis D. Brandeis).

As the use of the Internet expands, Americans might later regret any current lack of concern over privacy protection. For "[e]ven if Al Qaeda is somehow dismantled in the coming years [as a result of the USAPA], one suspects that technology's carefree days were also a victim of September 11."[334]

Cyndie Chang[*]

334. Koerner, *supra* note 306.

* I dedicate this to my parents, Mario and Mary, and my brothers, Kelvin and Jason for their continuous love and support, especially in my academic endeavors. I also thank the editors and staff of the Loyola of Los Angeles Entertainment Law Review for their diligent work. In particular, I thank Tom Werner, Leah Phillips Falzone, Brian E. Pellis, Scott Sterling, Benjamin Gemperle, and Carey Melton. Lastly, I also want to express great appreciation to the following individuals who encouraged and helped me develop the passion and substance for this Comment: Andrew Kahn, Jeanne Kuo, Craig Lang, Professor John Nockleby, and all my dear friends at Loyola Law School of Los Angeles.